INFORMATION AND CONTROL 8, 195–214 (1965)

An Algebraic Study of Group and Nongroup Error-Correcting Codes*

JAN-ERIK ROOS

Department of Mathematics, University of Lund, Sweden

In the first part of this paper linear, quadratic, . . . arbitrary n-block codes are studied by means of a technique using polynomials in n variables. By this method we get new proofs and refinements (for prime fields) of certain results of S. P. Lloyd and J. MacWilliams. In the last section it is shown how recent results of D. Slepian can be interpreted in terms of the Grothendieck ring of the category of linear codes over a fixed finite field. In this connection several conjectures are formulated.

INTRODUCTION

In this paper we present some new algebraic methods of studying arbitrary group and nongroup n-block codes.

In Section I a method is given of describing n-block codes by means of polynomials in n variables. This description is useful in studying quadratic, cubic, . . . codes that generalize the usual group (or linear) codes. As an application we deduce in Section II a formula which for linear codes over a prime field reduces to a generalization of a result of Jessie MacWilliams (1963) concerning the distribution of the weights of a linear code and its dual. As a further application we give in Section III a simple and purely algebraic treatment of closed-packed codes. Our results generalize those of S. P. Lloyd (1957). In particular, we obtain a duality theorem for closed-packed codes. This duality has for example the following consequences:

If a closed-packed $\leqq e$ error-correcting binary n-block code with more than one code point exists, then n *must be odd*. Further, *if* e *is odd, then* $n \equiv 3 \bmod 4$. (We suppose here that $e > 0$).

The last section is admittedly incomplete and it contains mostly conjectures about the Grothendieck group of the category of linear error-

* Work done by the author during service at the Research Institute of National Swedish Defense.

correcting codes. Our work here is inspired by the analogy between the results of Slepian (1960) and some recent advances in modern algebra (Borel-Serre, 1958; Grothendieck, 1958). For a good description of coding theory, the reader is referred to Peterson (1961).

I. DESCRIPTION OF CODES BY POLYNOMIALS

We will here restrict ourselves for simplicity to vector spaces V with explicit bases over the field $\mathbf{Z}/p\mathbf{Z}$ (p a prime) and arbitrary subsets of V (codes), although most results remain valid for vector spaces, over arbitrary finite fields and perhaps even for modules over a finite ring (using homological algebra).[1]

So let $V = F^n$ be the vector space of n-tuples of elements in $F = \mathbf{Z}/p\mathbf{Z}$. It is well-known that there are (at least) two different (for $p \neq 2$) interesting integral valued distances in V. If $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n) \in V$, then we can define

$$d_1(x, y) = \sum_{\alpha=1}^{n} | x_\alpha - y_\alpha |_1 ,$$

where for $\xi \in F$ we put

$$| \xi |_1 = \begin{cases} 0 & \text{if } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

and

$$d_2(x, y) = \sum_{\alpha=1}^{n} | x_\alpha - y_\alpha |_2$$

where for $\xi \in F = \mathbf{Z}/p\mathbf{Z}$ we put

$$| \xi |_2 = \text{the unique nonnegative representative}$$

$$\leqq p - 1 \quad \text{in the residue class } \xi.$$

Define

$$| x - y |_1 = d_1(x - y, 0) (= d_1(x, y))$$

and

$$| x - y |_2 = d_2(x - y, 0) (= d_2(x, y)).$$

[1] *Note added in proof:* Codes over a finite *ring* have recently been studied by E. F. Assmus and H. F. Mattson (*Inform. Control* **6**, 315–330 (1963)).

In both cases we have:

1. $| x + y | \leqq | x | + | y |$.

2. $| \alpha x | \equiv | \alpha | | x | \bmod p$ $(\alpha \in \mathbf{Z}/p\mathbf{Z})$.

3. $| x | = 0 \Leftrightarrow x = 0$.

The number $| x |$ is called the weight of x.

When $p = 2$ we have $d_1(x, y) = d_2(x, y) =$ number of α such that $x_\alpha \neq y_\alpha$. This is the usual Hamming distance.

It is clear that an arbitrary vector $x \in V$ can be uniquely described by $| x_1 |_2, \cdots, | x_n |_2$, i.e., by n integers $(i_1, \cdots, i_n)$ $(0 \leqq i_s \leqq p - 1)$. We will always abuse notation and write $x = (i_1, \cdots, i_n)$ instead of $x = (x_1, \cdots, x_n)$.

Now let C be a code in V. We associate with C a polynomial P_C in n variables as follows

$$P_C(X_1, \cdots, X_n) = \sum_{0 \leqq i_s \leqq p-1} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

where

$$a_{i_1} \cdots i_n = \begin{cases} +1 & \text{if } (i_1, \cdots, i_n) \text{ is a point of } C \\ 0 & \text{otherwise,} \end{cases}$$

so that

$$P_C(X_1, \cdots, X_n) = \sum_{(i_1, \cdots, i_n) \in C} X_1^{i_1} \cdots X_n^{i_n}$$

We thus obtain an integral polynomial $P_C \in \mathbf{Z}[X_1, \cdots, X_n]$, which is of degree $\leqq p - 1$ in each variable and which clearly determines C. Of course

$$P_C(X) = P_C(X, \cdots X) = \sum_{s=0}^{n(p-1)} \nu_s X^s,$$

where ν_s is the number of code vectors of weight s for the second norm.

The polynomial which represents all points of V is clearly

$$P_V(X_1, \cdots, X_n) = \prod_{s=1}^{n} (1 + X_s + X_s^2 + \cdots + X_s^{p-1}).$$

We will now study polynomials in $\mathbf{Z}[X_1, \cdots, X_n]$ modulo the ideal $(1 - X_1^p, \cdots, 1 - X_n^p)$ generated by $1 - X_1^p, \cdots, 1 - X_n^p$. If $Q \in \mathbf{Z}[X_1, \cdots, X_n]$, then there exists a unique polynomial $\tilde{Q}$ of degree

$\leqq p-1$ in each variable such that

$$Q \equiv \tilde{Q} \bmod (1 - X_1^p, \cdots, 1 - X_n^p)$$

This $\tilde{Q}$ will be called the *reduced polynomial of* Q. If $x = (i_1, \cdots, i_n)$ and $y = (j_1, \cdots, j_n)$, then the reduced polynomial of

$$X_1^{i_1} \cdots X_n^{i_n} \cdot X_1^{j_1} \cdots X_n^{j_n}$$

is

$$X_1^{k_1} \cdots X_n^{k_n},$$

where

$$x + y = (k_1, \cdots, k_n).$$

(Here we use the abuse of notation just mentioned.)

Now let

$$\begin{aligned}
\sigma_0(X_1, \cdots, X_n) &= 1 \\
\sigma_1(X_1, \cdots, X_n) &= X_1 + \cdots + X_n \\
&\cdots \\
\sigma_k(X_1, \cdots, X_n) &= \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k} \qquad (0 \leqq k \leqq n)
\end{aligned}$$

be the $n+1$ elementary symmetric polynomials in $X_1, X_2, \cdots X_n$, and let $x = (i_1, \cdots i_n) \in V$. Then clearly

$$\sigma_k\left(\sum_{s=1}^{p-1} X_1^s, \sum_{s=1}^{p-1} X_2^s, \cdots, \sum_{s=1}^{p-1} X_s^p\right) X_1^{i_1} \cdots X_n^{i_n}$$

is *after reduction a polynomial of the form* $P_{C'}$, where C' is the set of all points $y \in V$ such that

$$| x - y |_1 = k.$$

For example, the points of V corresponding to the polynomial

$$\sum_{\nu=1}^{n} \sum_{s=1}^{p-1} X_\nu^s$$

are exactly those points of V having distance 1 to the origin with respect to $|\cdot|_1$.

For the distance of type 2 the situation is a little more complicated. Let $\tau_k(X_1, \cdots, X_n)(0 \leqq k \leqq n(p-1))$ be the homogeneous part of

degree k of the polynomial

$$\prod_{s=1}^{n} (1 + X_s + X_s^2 + \cdots + X_s^{p-1}).$$

Then

$$\tau_k(X_1, \cdots, X_n) X_1^{i_1} \cdots X_n^{i_n} \equiv P_{C''}(X_1, \cdots, X_n) \bmod (1 - X_1^p, \cdots, 1 - X_n^p),$$

where C'' is the set of those $y \in V$ such that $| x - y |_2 = k$.

These results will be very useful in the study of closed-packed codes (cf. Section III).

II. LINEAR, QUADRATIC, CUBIC, ... CODES

Let $C \subset V$ be a linear code, e.g., a vector subspace of V. It is well-known that C can be described as the set of common zeros of a set of linear forms

$$\sum_{i=1}^{n} a_i^{(s)} x_i \qquad (s = 1, \cdots, n), \qquad (a_i^{(s)} \in F).$$

The set of all such forms that are zero on C constitutes a linear subspace of $\mathrm{Hom}_F(V, F)$ = the set of all linear functions $V \to F$, with its natural vector space structure. If we give $\mathrm{Hom}_F(V, F)$ the dual basis of the canonical basis in $V = F^n$, then we get in this way a linear code $\hat{C} \subset \mathrm{Hom}_F(V, F)$, *the dual code of* C, and it is easy to see that C is the dual of $\hat{C}$.

Now suppose more generally that C is the set of common zeros of a set of quadratic-linear forms

$$\sum_i a_i^{(s)} x_i + \sum_{i,k} a_{ik}^{(s)} x_i x_k .$$

Then the set of all such forms that are zero on C form a linear subspace in $\mathrm{Hom}_F^2(V, F)$ = the set of all linear-quadratic functions $V \to F$. By a linear-quadratic function $V \to F$ we mean a map $V \xrightarrow{f} F$ such that for every fixed y,

$$V \ni x \to f(x + y) - f(x) - f(y) \in F$$

is an element of $\mathrm{Hom}_F(V, F)$ and such that for a suitable $\tilde{f} \in \mathrm{Hom}_F(V, F)$ we have

$$(f - \tilde{f})(ax) = a^2 (f - \tilde{f})(x), \qquad a \in F.$$

Now the situations for $p = 2$ and $p \neq 2$ are a little different. Suppose first than $p \neq 2$. Then it is easy to see that

$$V \xrightarrow{\epsilon_{ik}} F : (x_1, \cdots, x_n) \to x_i x_k \in F \qquad (i \leqq k)$$

$$V \xrightarrow{\epsilon_i} F : (x_1, \cdots, x_n) \to x_i \in F \qquad (1 \leqq i \leqq n)$$

form a basis for $\mathrm{Hom}_F{}^2(V, F)$ so that this space has dimension

$$\binom{n}{1} + \left(\binom{n}{1} + \binom{n}{2}\right) = \frac{n(n+3)}{2}$$

over F. The linear subspace of all $f \in \mathrm{Hom}_F{}^2(V, F)$ that are zero on C is called $\hat{C}^2$ and it is clearly a linear code in $\mathrm{Hom}_F{}^2(V, F)$ if we use the basis ϵ_{ik} , ϵ_i . This code is called the dual of C. It is easy to see that the set of elements in V that make all $f \in \hat{C}^2$ zero is just C.

Thus C is *completely determined by a linear code* in the space of linear-quadratic functions. We will call C a quadratic code. In a similar way we can define cubic, . . . codes, but we will stick to the quadratic code for simplicity in notation. If $p = 2$, the dimension of $\mathrm{Hom}_F{}^2(V, F)$ is n units lower since we can take away all $\epsilon_{ii}(x_i{}^2 = x_i$ in $\mathbf{Z}/2\mathbf{Z})$. The modifications necessary in this case are trivial, and we will only formulate the results for $p \neq 2$.

Remark: For simplicity we have only considered quadratic codes that pass through the origin. But any code could be translated by a vector so as to pass through the origin. This does not change the distances between code-points.

Now

$$P_C(X_1, \cdots, X_n) = \sum_{0 \leqq i_s \leqq p-1} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

and

$$P_{\hat{C}^2}(X_1, \cdots, X_n) = \sum_{\xi = (\cdots \xi_r \cdots \xi_{st} \cdots) \in \hat{C}^2} X_1^{\xi_1} \cdots X_n^{\xi_n} \cdots X_{st}^{\xi_{st}} \cdots$$

are defined. What are the relations between these two polynomials? We will first prove the formula

$$P_{\hat{C}^2}(1, \cdots, 1) a_{i_1 \cdots i_n} = \sum_{\xi \in \hat{C}^2} \exp\left[\frac{2\pi i}{p} \left(\sum_s i_s \xi_s + \sum_{s \leqq t} i_s \, i_t \, \xi_{st}\right)\right] \qquad (1)$$

Here $(i_1 \cdots i_n)$ is a fixed set of indices. (Of course $P_{\hat{C}^2}(1, \cdots, 1)$ can be written more simply as $p^{\dim_F \hat{C}^2}$, and it is also equal to $| \hat{C}^2 |$ where for *any* code C' we introduce $| C' |$ = number of points in C'.)

According to the definition $(i_1, \cdots, i_n) \in C \Leftrightarrow$

$$\sum_s i_s\xi_s + \sum_{s \leqq t} i_s i_t \xi_{st} \equiv 0 \pmod p, \quad \forall(\xi_1, \cdots, \xi_n, \cdots, \xi_{st}, \cdots) \in \hat{C}^2.$$

Thus if $(i_1, \cdots, i_n) \in C$, the right-hand side of (1) becomes

$$\sum_{\xi \in \hat{C}^2} 1 = P_{\hat{C}^2}(1, \cdots, 1)$$

and this is equal to the left-hand side since $a_{i_1 \cdots i_n} = 1$.

Suppose now that $(i_1, \cdots, i_n) \notin C$. Then to the left of (1) we have 0. To the right we know that there exists $(\xi_1^*, \cdots, \xi_n^*, \cdots, \xi_{st}^*, \cdots) \in \hat{C}^2$ such that

$$\sum_s i_s\xi_s^* + \sum_{s \leqq t} i_s i_t \xi_{st}^* \not\equiv 0 \pmod p. \tag{2}$$

Let $\hat{C}^2(s)$ be the set of all $\xi \in \hat{C}^2$ such that the sum (2) is $\equiv s \bmod p$, $(0 \leqq s \leqq p-1)$. Since $\hat{C}^2$ is a vector space, $y \in \hat{C}^2 \Rightarrow \lambda y \in \hat{C}^2$ for $\lambda \in F$, and it is clear that multiplication with the $0 \neq \lambda \in F$ induces a one-one correspondence between the $\hat{C}^2(s)$ for $0 < s \leqq p-1$. Now suppose that $\xi^* \in \hat{C}^2(s^*)(0 < s^* \leqq p-1)$. Then

$$\hat{C}^2(0) \ni \xi \to \xi + \xi^* \in \hat{C}^2(s^*)$$

is a one-one correspondence too and so the disjoint subsets $\{\hat{C}^2(s)\}_{0 \leqq s \leqq p-1}$ of $\hat{C}^2$ cover $\hat{C}^2$ and have the same number of elements, say N. Then the right-hand side of (1) becomes

$$N \sum_{s=0}^{p-1} \exp\left(\frac{2\pi i s}{p}\right) = 0,$$

and so (1) is proved.

Now multiply (1) by $X_1^{i_1} \cdots X_n^{i_n}$ and sum over all $(i_1, \cdots, i_n)$. We get

THEOREM 1. *If C is a quadratic code, $\hat{C}^2$ its dual, then*

$$|\hat{C}^2| P_C(X_1, \cdots, X_n) = \sum_{\xi \in \hat{C}^2} \sum_{(i_1 \cdots i_n) \in V} X_1^{i_1} \cdots X_n^{i_n} \cdot \exp\left[\frac{2\pi i}{p}\left(\sum \xi_s i_s + \sum \xi_{st} i_s i_t\right)\right].$$

This theorem gives a description of C in terms of the linear code $\hat{C}^2$. Un-

fortunately the sum

$$\sum_{\substack{i_1 \cdots i_n \\ 0 \leqq i_s \leqq p-1}} X_1^{i_1} \cdots X_n^{i_n} \exp\left[\frac{2\pi i}{p}\left(\sum \xi_s i_s + \sum_{s \leqq t} \xi_{st} i_s i_t\right)\right]$$

is rather difficult to evaluate. It should be considered as a sort of weighted generalized Gaussian sum.

If we had done our reasoning for a linear code (p arbitrary) then we would have obtained

$$|\hat{C}| P_C(X_1, \cdots, X_n) = \sum_{\xi \in \hat{C}} \sum_{0 \leqq i_s \leqq p-1} X_1^{i_1} \cdots X_n^{i_n} \exp\left[\frac{2\pi i}{p}\left(\sum_s \xi_s i_s\right)\right].$$

Let us now show how this formula can be used to generalize a result of Jessie MacWilliams (1963) for $p = 2$. In this case we obtain

$$\begin{aligned} |\hat{C}| P_C(X_1, \cdots, X_n) &= \sum_{\xi \in \hat{C}} \sum_{0 \leqq i_s \leqq 1} ((-1)^{\xi_1} X_1)^{i_1} \cdots ((-1)^{\xi_n} X_n)^{i_n} \qquad (3) \\ &= \sum_{\xi \in \hat{C}} (1 + (-1)^{\xi_1} X_1) \cdots (1 + (-1)^{\xi_n} X_n). \end{aligned}$$

But

$$1 + (-1)^{\xi_s} X_s = \left(\frac{1 - X_s}{1 + X_s}\right)^{\xi_s} (1 + X_s), \text{ if } \xi_s = 0 \text{ or } 1,$$

so that the last member of (3) is

$$\prod_{s=1}^{n} (1 + X_s) \cdot \sum_{\xi \in \hat{C}} \left(\frac{1 - X_1}{1 + X_1}\right)^{\xi_1} \cdots \left(\frac{1 - X_n}{1 + X_n}\right)^{\xi_n}$$

$$= \prod_{s=1}^{n} (1 + X_s) P_{\hat{C}}\left(\frac{1 - X_1}{1 + X_1}, \cdots, \frac{1 - X_n}{1 + X_n}\right).$$

Thus,

COROLLARY. *If C is a linear code in $(\mathbf{Z}/2\mathbf{Z})^n$ and $\hat{C}$ its dual, then we have the following relation between P_C and $P_{\hat{C}}$*

$$|\hat{C}| P_C(X_1, \cdots, X_n) = \prod_{j=1}^{n} (1 + X_j) P_{\hat{C}}\left(\frac{1 - X_1}{1 + X_1}, \cdots, \frac{1 - X_n}{1 + X_n}\right).$$

In particular, if we put $X_1 = X_2 = \cdots = X_n = X$, we obtain

$$|\hat{C}| P_C(X) = (1 + X)^n P_{\hat{C}}\left(\frac{1 - X}{1 + X}\right),$$

which is exactly the result of Jessie MacWilliams (1963) (for $p = 2$).

Remark: Quadratic, cubic, . . . codes should be interesting for the following reason: If the best group code of a given size for a given channel is not optimum, then one might hope that the best quadratic, or cubic, . . . or . . . codes (with a suitable decoding procedure) are optimum. It remains to work out explicit examples.

III. THEORY OF CLOSED-PACKED ERROR-CORRECTING CODES

Recall that a subset $C \subset V = F^n$ is said to be a closed-packed $\leqq e$ error-correcting code with respect to a given distance on V if the solid spheres with radius e (for the given distance) and centered at the code points are disjoint and cover V.

Now by results of Section I we can explicitly describe polynomials

$$\sigma_k\left(\sum_{s=1}^{p-1} X_1^s, \cdots, \sum_{s=1}^{p-1} X_n^s\right) X_1^{i_1} \cdots X_n^{i_n} \qquad (')$$

resp.

$$\tau_k(X_1, \cdots, X_n) X_1^{i_1} \cdots X_n^{i_n} \qquad ('')$$

which, reduced, give the $P_{C'}$ (resp. $P_{C''}$) corresponding to the set C' (resp. C'') of points of V of distance (with respect to $|\cdot|_1$ resp. $|\cdot|_2$) exactly k from a given point $x = (i_1, \cdots, i_n)$. Thus if we take the sum of all the polynomials $(')$ (resp. $('')$) for all code points x and all $k (0 \leqq k \leqq e)$ we get two polynomials Q' and Q'', and it is clear that we obtain after reduction of Q' (resp. Q'') the polynomial that corresponds to exactly all points of V if and only if C is closed-packed with respect to $|\cdot|_1$ (resp. $|\cdot|_2$). Thus the following two theorems are immediate (cf. Section I):

THEOREM 2. *A necessary and sufficient condition for $C \subset V = F^n$ to be a closed-packed $\leqq e$ error-correcting code for the distance of the first type, is that the corresponding polynomial P_C should satisfy the following congruence:*

$$\sum_{k=0}^{e} \sigma_k\left(\sum_{s=1}^{p-1} X_1^s, \cdots, \sum_{s=1}^{p-1} X_n^s\right) \cdot P_C(X_1, \cdots, X_n) \equiv \prod_{t=1}^{n}\left(\sum_{s=0}^{p-1} X_t^s\right) \mod (1 - X_1^p, \cdots, 1 - X_n^p) \qquad (4)$$

where σ_k is the kth elementary symmetric polynomial.

THEOREM 3. *A necessary and sufficient condition for $C \subset V = F^n$ to be a closed-packed $\leqq e$ error-correcting code for the distance of the second type, is that the corresponding polynomial P_C should satisfy the following*

congruence

$$\sum_{k=0}^{e} \tau_k(X_1, \cdots, X_n) \cdot P_C(X_1, \cdots, X_n) \equiv \prod_{i=1}^{n} \left(\sum_{s=0}^{p-1} X_i^s \right) \mod (1 - X_1^p, \cdots, 1 - X_n^p)$$

where τ_k is defined in Section I (it is symmetric in $X_1, \cdots, X_n$).

We will only analyze the simpler formula (4). Now the linear isometric automorphisms of $(V, |\cdot|_1)$ are composed of

1. The maps

$$e_i \to e_{\sigma(i)} (1 \leqq i \leqq n), \ (\{e_i\} \text{ is the canonical basis of } V)$$

where $\sigma \in \mathfrak{S}_n$, the symmetric group of n letters.

2. The maps $e_i \to \lambda_i e_i (1 \leqq i \leqq n)$, where $0 \neq \lambda_i \in F$.

The first factor and the second member of (4) remain invariant under such automorphisms (the transformed C is also closed-packed). Let us take the average of all formulas (4) over all automorphisms. Since

$$P_C(X_1, \cdots, X_n) = \sum_{(i_1, \cdots, i_n) \in C} X_1^{i_1} \cdots X_n^{i_n}$$

we obtain

$$\sum_{k=0}^{e} \sigma_k \left(\sum_{t=1}^{p-1} X_1^t, \cdots, \sum_{t=1}^{p-1} X_n^t \right) \frac{1}{n!(p-1)^n} \cdot \sum_{(i_1, \cdots, i_n) \in C} \sum_{\substack{1 \leqq k_s \leqq p-1 \\ \sigma \in \mathfrak{S}_n}} X_{\sigma(1)}^{i_1 k_1} \cdots X_{\sigma(n)}^{i_n k_n} \equiv \prod_{s=0}^{n} \left(\sum_{t=0}^{p-1} X_s^t \right) \tag{5}$$

$$\mod (1 - X_1^p, \cdots, 1 - X_n^p)$$

in $\mathbf{Q}[X_1, \cdots, X_n]$. But

$$\sum_{1 \leqq k_s \leqq p-1} X_s^{i_s k_s} \equiv \begin{cases} X_s + X_s^2 + \cdots + X_s^{p-1}, & \text{if } i_s \neq 0 \\ p - 1 \text{ otherwise} \end{cases} \tag{6}$$

Now put

$$\nu_s = \sum_{i_1 \cdots i_n} 1$$

where the sum is taken over those $(i_1 \cdots i_n) \in C$ such that exactly s of them are $\neq 0$. (ν_s = the number of code points of weight s for the distance $|\cdot|_1$.) Then using (6) we obtain

$$\sum_{0 \leqq i_s \leqq p-1} a_{i_1 \cdots i_n} \sum_{0 \leqq k_s \leqq p-1} X_1^{i_1 k_1} \cdots X_n^{i_n k_n} \equiv \sum_{s=0}^{n} \nu_s \frac{n!(p-1)^{n-s}}{\binom{n}{s}}$$

$$\cdot\sigma_s\left(\sum_{t=1}^{p-1} X_1^t, \cdots, \sum_{t=1}^{p-1} X_n^t\right) \bmod (1 - X_i^p, \cdots, 1 - X_n^p),$$

so that (5) can finally be written

$$\sum_{k=0}^{e} \sigma_k\left(\sum_{t=1}^{p-1} X_1^t, \cdots, \sum_{t=1}^{p-1} X_n^t\right) \sum_{s=0}^{n} \nu_s \frac{\sigma_s\left(\sum_{t=1}^{p-1} X_1^t, \cdots, \sum_{t=1}^{p-1} X_n^t\right)}{\binom{n}{s}(p-1)^s} \tag{7}$$

$$\equiv \prod_{s=1}^{n}\left(\sum_{t=0}^{p-1} X_s^t\right) \bmod (1 - X_1^p, \cdots, 1 - X_n^p).$$

Now this congruence must become an *identity* if we put every X_i equal to some pth root of unity x_i (for then $x_i^p = 1$). Of course, *for such an* x_s we have

$$x_s + \cdots + x_s^{p-1} = \begin{cases} p - 1, & \text{if } x_s = 1, \\ -1, & \text{if } x_s \neq 1. \end{cases}$$

Thus if k of the x_i's are $= +1$ and the rest are pth roots of unity $\neq 1$, then $\sigma_s(x_1 + \cdots + x_1^{p-1}, \cdots, x_n + \cdots + x_n^{p-1}) =$ the coefficient of X^s in $(1 + (p-1)X)^k(1 - X)^{n-k}$, so if we introduce polynomials $\varphi_k^{(p-1)}(n, \xi)$ in the variable ξ by

$$(1 + (p-1)X)^{\xi}(1 - X)^{n-\xi} = \sum_{k=0}^{\infty} \varphi_k^{(p-1)}(n, \xi)X^k, \tag{8}$$

then we obtain from (7)

$$\left(\sum_{s=0}^{e} \varphi_s^{(p-1)}(n, k)\right) \sum_{s=0}^{n} \nu_s \frac{\varphi_s^{(p-1)}(n, k)}{\binom{n}{s}(p-1)^s} = \begin{cases} 0, & 0 \leqq k < n \\ p^n, & k = n \end{cases} \tag{9}$$

Since $\varphi_s^{(p-1)}(n, n) = \binom{n}{s}(p-1)^s$, formula (9) for $k = n$ gives

$$\left[\sum_{s=0}^{e} \binom{n}{s}(p-1)^s\right] \cdot \left[\sum_{s=0}^{n} \nu_s\right] = p^n,$$

which is exactly the (generalized) Hamming condition.

The other formulas (9) are analogous to this condition and we will show that they imply in fact a generalization of the results of S. P. Lloyd (1957). First it is easy to prove as in Lloyd (1957), using the

definition (8), that

$$\sum_{s=0}^{e} \varphi_s^{(p-1)}(n, \xi) = \varphi_e^{(p-1)}(n-1, \xi)$$

It is also easy to generalize Appendix B of Lloyd (1957) to the following formulas

$$\frac{\varphi_s^{(p-1)}(n, k)}{\binom{n}{s}} = (-1)^{s-k} \frac{\varphi_k^{(p-1)}(n, s)}{\binom{n}{k}}, \qquad s, k \text{ integers in } [0, n].$$

If we use these two results, then (9) can be rewritten as

$$\varphi_e^{(p-1)}(n-1, k) \left(\sum_{s=0}^{n} \nu_s \frac{(-1)^s}{(p-1)^s} \varphi_k^{(p-1)}(n, s) \right) = \delta_{kn} p^n \binom{n}{k} (-1)^n, \qquad k = 0, 1, 2, \cdots, n. \tag{10}$$

But since $\varphi_k^{(p-1)}(n, s) = \text{coeff}_{X^k} (1 + (p-1)X)^s (1 - X)^{n-s}$, formula (10) can be transformed into

$$\varphi_e^{(p-1)}(n-1, k) \, \text{coeff}_{X^k} \left[(X-1)^n G_C \left(\frac{X + 1/(p-1)}{X-1} \right) \right] = \delta_{kn} p^n, \tag{11}$$

where $G_C(Y) = \sum_{s=0}^{n} \nu_s Y^s$. Thus if $\varphi_e^{(p-1)}(n-1, k) \neq 0$ for $k < n$, then the corresponding coefficient

$$\text{coeff}_{X^k} \left[(X-1)^n G_C \left(\frac{X + 1/(p-1)}{X-1} \right) \right] = 0.$$

I will now show that (11) forces the e zeros of $\varphi_e^{(p-1)}(n-1, \xi)$ to be different integers in $[0, n-1]$. Let $0 \leqq \xi_1 < \xi_2 < \cdots < \xi_t < n (t \leqq e)$ be the different integer zeros of $\varphi_e^{(p-1)}(n-1, \xi)$ in this interval. (A priori there could be no such zeros. Then we put $t = 0$ and use no ξ_s's). I claim that $t = e$. Since

$$(X-1)^n G_C \left(\frac{X + 1/(p-1)}{X-1} \right)$$

is a polynomial of degree $\leqq n$, we get from (11), if we put

$$Y = [X + 1/(p-1)]/(X-1)$$

and simplify:

$$G_C(Y) = \sum_{s=1}^{t} A_s(1 + (p-1)Y)^{\xi_s}(1-Y)^{n-\xi_s} + A_n(1 + (p-1)Y)^n,$$

where (12)

$$A_n = \frac{1}{\varphi_e^{(p-1)}(n-1, n)},$$

and the A_s are certain constants.

Since C is a closed-packed $\leqq e$ error-correcting code, there is at most one code point of weight $\leqq e$. Suppose that this weight is $\gamma (0 \leqq \gamma \leqq e)$. We will show that G_C depends only on γ. In fact, since

$$G_C(Y) = Y^\gamma + \text{terms of degree} \geqq e + 1,$$

we get from (12)

$$\sum_{s=1}^{t} A_s \varphi_k^{(p-1)}(n, \xi_s) + A_n \varphi_k(n, n) + \delta_{k\gamma}(-1) = 0, \quad 0 \leqq k \leqq e,$$

$$\sum_{s=1}^{s} A_s(1 + (p-1)Y)^{\xi_s}(1-Y)^{n-\xi_s} + A_n(1 + (p-1)Y)^n + G_C(Y)(-1) = 0. \tag{13}$$

Suppose first that $\gamma = e$. (By adding a suitable vector to C we can obtain such a code.) If $t < e$ then the $t + 1$ equations

$$\sum_{s=1}^{t} A_s \varphi_k^{(p-1)}(n, \xi_s) + A_n \varphi_k(n, n) = 0, \quad 0 \leqq k \leqq t$$

for the unknowns A_s have a nontrivial solution ($A_n \neq 0$!), and so the determinant must be zero. But this gives

$$\begin{vmatrix} \varphi_0^{(p-1)}(n, \xi_1) & \cdots & \varphi_0^{(p-1)}(n, \xi_t) & \varphi_0^{(p-1)}(n, n) \\ \vdots & & \vdots & \vdots \\ \varphi_t^{(p-1)}(n, \xi_1) & \cdots & \varphi_t^{(p-1)}(n, \xi_t) & \varphi_t^{(p-1)}(n, n) \end{vmatrix} = 0,$$

which is impossible since the determinant can be transformed into a van der Monde determinant of $\xi_1 < \cdots < \xi_t < n$. Thus $t = e$ and so the $e + 2$ equations (13) for the unknowns $A_1, \cdots, A_e, A_n, (-1)$ have a nontrivial solution. Thus the corresponding determinant is zero,

and we obtain for a C with minimum weight γ:

$$\begin{vmatrix} \varphi_0^{(p-1)}(n,\xi_1) & \cdots & \varphi_0^{(p-1)}(n,\xi_e) & \varphi_0^{(p-1)}(n,n) & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ \varphi_\gamma^{(p-1)}(n,\xi_1) & \cdots & \varphi_\gamma^{(p-1)}(n,\xi_e) & \varphi_\gamma^{(p-1)}(n,n) & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ \varphi_e^{(p-1)}(n,\xi_1) & \cdots & \varphi_e^{(p-1)}(n,\xi_e) & \varphi_e^{(p-1)}(n,n) & 0 \\ (1+(p-1)Y)^{\xi_1}(1-Y)^{n-\xi_1} & \cdots & (1+(p-1)Y)^{\xi_e}(1-Y)^{n-\xi_e} & (1+(p-1)Y)^n & G_C(Y) \end{vmatrix} = 0, \quad (14)$$

which uniquely determines G_C, so that the notation $G^{(\gamma)}$ is in order. The formula (14) gives for $p = 2$ a result which is equivalent to a result of S. P. Lloyd (1957) although not identical in form. It should be remarked that (14) is suitable for calculations. Suppose for example that $e = 1$. Then

$$\varphi_1^{(p-1)}(n-1,\xi) = \xi \cdot p - (n-1),$$

so that $\xi_1 = (n-1)/p$ must be an integer and $G^{(0)}$ respective $G^{(1)}$ are given by

$$\begin{vmatrix} 1 & 1 & 1 \\ -1 & n(p-1) & 0 \\ (1+(p-1)Y)^{(n-1)/p}(1-Y)^{n-(n-1)/p} & (1+(p-1)Y)^n & G^{(0)}(Y) \end{vmatrix} = 0,$$

and

$$\begin{vmatrix} 1 & 1 & 0 \\ -1 & n(p-1) & 1 \\ (1+(p-1)Y)^{(n-1)/p}(1-Y)^{n-(n-1)/p} & (1+(p-1)Y)^n & G^{(1)}(Y) \end{vmatrix} = 0,$$

which are the well-known formulas for the distribution of weights in a Hamming code (Peterson, 1961, p. 68).

Now we will prove a duality theorem for the G_C when $p = 2$.

THEOREM 4. *Let C be a closed-packed $\leqq e$ error-correcting code with more than one code point in $V = F^n$ ($F = \mathbf{Z}/2\mathbf{Z}$). Then*

$$G_C(X) = X^n G_C(1/X),$$

i.e., $\nu_s = \nu_{n-s}$, *where ν_s = the number of code points of weight s in C.*

Proof: If we add the vector $(1, \cdots, 1)$ to C then we will get a new

closed-packed code C' with polynomial

$$G_{C'}(X) = X^n G_C(1/X). \tag{15}$$

If C is of type γ, then let C' be of type γ'. In this way we obtain a one-one mapping $\gamma \to \gamma'$ of $[0, e]$ onto itself, with $\gamma'' = \gamma$, and our theorem is clearly equivalent to the assertion $\gamma' = \gamma$. Now (15) can be written

$$G^{(\gamma')}(X) = X^n G^{(\gamma)}(1/X),$$

and according to (14) (for $p = 2$), this is equivalent to the relations: ($\varphi_\gamma^{(1)}(n, \xi)$ is written $\varphi_\gamma(n, \xi)$)

$$\frac{\varphi_{\gamma'}(n, \xi_\beta)}{\varphi_{\gamma'}(n, n)} = (-1)^{n-\xi_\beta} \frac{\varphi_\gamma(n, \xi_\beta)}{\varphi_\gamma(n, n)}, \quad 1 \leqq \beta \leqq e, \tag{16}$$

so that in particular

$$\frac{\varphi_{0'}(n, \xi_\beta)}{\varphi_{0'}(n, n)} = (-1)^{n-\xi_\beta}. \tag{17}$$

But from (16) we have

$$\sum_{\gamma' \neq 0'} \varphi_{\gamma'}(n, \xi_\beta) = (-1)^{n-\xi_\beta} \sum_{\gamma \neq 0} \varphi_\gamma(n, \xi_\beta) \frac{\varphi_{\gamma'}(n, n)}{\varphi_\gamma(n, n)}. \tag{18}$$

The left side of (18) is equal to

$$\sum_{0 \leqq \gamma' \leqq e} \varphi_{\gamma'}(n, \xi_\beta) - \varphi_{0'}(n, \xi_\beta).$$

But the first sum is equal to $\varphi_e(n - 1, \xi_\beta)$ and thus zero. As for $-\varphi_{0'}(n, \xi_\beta)$, it is equal to $-(-1)^{n-\xi_\beta}\varphi_{0'}(n, n)$, according to (17). Thus (18) can be written

$$\sum_{0 < \gamma \leqq e} \varphi_\gamma(n, \xi_\beta) \frac{\varphi_{\gamma'}(n, n)}{\varphi_\gamma(n, n)} + \varphi_{0'}(n, n) = 0, \qquad 1 \leqq \beta \leqq e.$$

In other words the polynomials

$$\sum_{\gamma \neq 0} \varphi_\gamma(n, \xi) \frac{\varphi_{\gamma'}(n, n)}{\varphi_\gamma(n, n)} + \varphi_{0'}(n, n)$$

and $\varphi_e(n - 1, \xi)$ have the same zeros (they are of the same degree). Thus we get an identity

$$\sum_{0 < \gamma \leqq e} \varphi_\gamma(n, \xi) \frac{\varphi_{\gamma'}(n, n)}{\varphi_\gamma(n, n)} + \varphi_{0'}(n, n) = K\varphi_e(n - 1, \xi), \quad (K = \text{a constant}) \tag{19}$$

Now put $\xi = n$ in (19). This gives $K = 1$, and so we obtain upon identifying the coefficients of highest degree in (19):

$$\frac{\varphi_{e'}(n, n)}{\varphi_e(n, n)} = 1$$

or

$$\binom{n}{e} = \binom{n}{e'}. \tag{20}$$

But $0 \leqq e' \leqq e$. Further, we have more than one code point and thus $2e + 1 \leqq n$. But under these conditions (20) can only be valid if $e = e'$ and continuing the identification (19) (with $K = 1$), we get $\gamma = \gamma'$ for all γ and the theorem is proved.

COROLLARY. *Under the conditions of Theorem* 4, *n must be odd and the zeros of* $\varphi_e(n - 1, \xi)$ *must be different odd integers. If, moreover, e is odd then* $n \equiv 3 \bmod 4$. (We suppose here that $e > 0$).

Proof: From (17) we get using $0' = 0$, that $(-1)^{n-\xi_\beta} = 1$ for all zeros of $\varphi_e(n - 1, \xi)$. But

$$\varphi_e(n - 1, \xi) = (-1)^e \varphi_e(n - 1, n - 1 - \xi) \tag{21}$$

so that $n - 1 - \xi_\beta$ is also a zero and so $(-1)^{\xi_\beta + 1} = 1$. Thus ξ_β is odd and n is odd, proving the first part of the corollary. If e is odd then according to (21), $(n - 1)/2$ is a zero of $\varphi_e(n - 1, \xi)$ and is thus an odd integer, proving the second part.

Remark: The result is sharp: For the Golay code (Peterson, 1961, pp. 70, 140, 167) we have $n = 23$, e odd ($e = 3$) and $23 - 3 = 4 \cdot 5$.

IV. THE GROTHENDIECK RING OF THE CATEGORY OF LINEAR CODES

Let F be the field $\mathbf{Z}/p\mathbf{Z}$. Obviously a linear code can be described as a triple

$$\mathbf{E} = (V, \{\varphi_\alpha\}, C),$$

where V is a finite-dimensional vector space over F, $\{\varphi_\alpha\}$ is an explicit basis for this space, and C is a linear subspace. The sum $\mathbf{E} \dotplus \mathbf{E}'$ of two codes $\mathbf{E}$ and $\mathbf{E}' = (V', \{\varphi_\beta'\}, C')$ is defined as the code

$$\mathbf{E} \dotplus \mathbf{E}' = (V \dotplus V', \{(\varphi_\alpha, 0)\} \cup \{(0, \varphi_\beta')\}, C \dotplus C'),$$

where $V \dotplus V'$ is the direct sum of vector spaces. For every $\mathbf{E}$ we can

define a distance in V by

$$|x| = \sum |x_\alpha|_2 ,$$

where x_α is defined by $x = \sum x_\alpha \varphi_\alpha$.

Two codes $\mathbf{E}$ and $\mathbf{E}'$ are said to be isomorphic (notation $\mathbf{E} \tilde{\to} \mathbf{E}'$) if there exists a linear isomorphism $V \tilde{\to} V'$ which maps C isomorphically onto C' and leaves the distance invariant.

$$|f(x)| = |x|.$$

(f then induces a one-one map of $\{\varphi_\alpha\}$ onto $\{\varphi_\beta'\}$). In analogy with certain constructions of Grothendieck (Borel-Serre, 1958) concerning the categories involved in the statement of the Grothendieck-Riemann-Roch theorem, it is now natural to make the following construction.

Let $L(F)$ be the *free abelian group* generated by all the different isomorphy classes of codes $\mathbf{E}$. We denote the isomorphy class of $\mathbf{E}$ by $[\mathbf{E}]$. Consider the subgroup $S(F)$ of $L(F)$ generated by all elements of the form

$$[\mathbf{E}] - [\mathbf{E}_1] - [\mathbf{E}_2],$$

where

$$\mathbf{E} \tilde{\to} \mathbf{E}_1 \dotplus \mathbf{E}_2 .$$

The quotient group $L(F)/S(F)$ is denoted by $K = K(F)$ and it will be called the Grothendieck group of the category of error-correcting group-codes over F.

Now we will introduce further algebraic structure on $K(F)$. The *tensorproduct* $\mathbf{E}_1 \otimes_F \mathbf{E}_2$ of two codes $\mathbf{E}_1$ and $\mathbf{E}_2$ is defined by

$$\mathbf{E}_1 \otimes_F \mathbf{E}_2 = (V_1 \otimes_F V_2 , \{\varphi_{1\alpha} \otimes \varphi_{2\beta}\}, C_1 \otimes_F C_2).$$

Since

$$\mathbf{E} \tilde{\to} \mathbf{E}' \Rightarrow \mathbf{E} \otimes \mathbf{E}_2 \tilde{\to} \mathbf{E}' \otimes \mathbf{E}_2 , \tag{22}$$

and similarly for the second factor, it is possible to define a product in $L(F)$ by

$$[\mathbf{E}_1] \cdot [\mathbf{E}_2] = [\mathbf{E}_1 \otimes_F \mathbf{E}_2].$$

In this way, L becomes a commutative ring with unity

$$(F, \{1\}, F) \qquad (1 \text{ is the unit in } F)$$

Further it follows from the formula

$$\mathbf{E}_1 \otimes (\mathbf{E}_2 \dot{+} \mathbf{E}_3) \tilde{\to} (\mathbf{E}_1 \otimes \mathbf{E}_2) \dot{+} (\mathbf{E}_1 \otimes \mathbf{E}_3)$$

and (22) that $S(F)$ is an ideal in this ring so that $K(F)$ becomes a commutative ($\mathbf{E}_1 \otimes \mathbf{E}_2 \tilde{\to} \mathbf{E}_2 \otimes \mathbf{E}_1$!) *ring with identity*. But there is still more structure on $K(F)$; it has the structure of a λ-ring (Borel-Serre, 1958; Grothendieck, 1958) which will be defined now.

Let us define the kth exterior product of a code by

$$\bigwedge^k \mathbf{E} = (\bigwedge^k V, \{\varphi_{\alpha_1} \wedge \cdots \wedge \varphi_{\alpha_k}\}, \bigwedge^k C), \alpha_1 < \cdots < \alpha_k ,$$

where $\bigwedge^k V$ is the kth exterior product of the vector space V and $\bigwedge^k C$ is embedded in $\bigwedge^k V$ by means of $\bigwedge^k i$, where $C \xrightarrow{i} V$ is the canonical injection. In this way we obtain (nonlinear!) operations

$$L(F) \xrightarrow{\Lambda^k} L(F) : [\mathbf{E}] \to [\bigwedge^k \mathbf{E}].$$

Let $\lambda^k([\mathbf{E}])$ be the image of $[\bigwedge^k \mathbf{E}]$ in $K(F)$. Now let $K[[T]]_1{}^*$ be the *multiplicative group* of those formal power series in the indeterminate T with coefficients in the ring $K = K(F)$, which have the forms

$$1 + a_1 T + a_2 T^2 + \cdots ,$$

where 1 is the unit in $K(F)$ (and $a_i \in K(F)$) (this is an abelian group!). It is clear that we get a map

$$L(F) \xrightarrow{\lambda_T} K[[T]]_1{}^*$$

by

$$[\mathbf{E}] \to \sum_{k \geqq 0} \lambda^k([\mathbf{E}]) T^k$$

$$(\lambda^0([\mathbf{E}]) = 1).$$

From the formula

$$\bigwedge^k (\mathbf{E}_1 \dot{+} \mathbf{E}_2) \tilde{\to} \dot{\sum_{s+t=k}} \bigwedge^s \mathbf{E}_1 \otimes \bigwedge^t \mathbf{E}_2 ,$$

it follows that

$$\lambda_T([\mathbf{E}_1 \dot{+} \mathbf{E}_2]) = \lambda_T([\mathbf{E}_1]) \cdot \lambda_T([\mathbf{E}_2]),$$

so that λ_T passes to the quotient and defines a homomorphism,

$$K(F) \xrightarrow{\lambda_T} K[[T]]_1{}^*. \tag{23}$$

Now we *define* $\lambda^k(x)$ for $x \in K(F)$ as the coefficient of T^k in $\lambda_T(x)$.

In this way we get (nonlinear!) applications

$$K(F) \xrightarrow{\lambda^s} K(F),$$

which have certain properties that are easy to make explicit ((23) is a homomorphism ...).

THEOREM 5. *Let $K(F)$ be the Grothendieck group of the category of linear codes over F. Then the tensor product of codes gives $K(F)$ the structure of a commutative ring with a unit. Further the exterior product of codes defines on $K(F)$ the* structure of a λ-ring. *By this we mean that there exist (nonlinear!) applications $\lambda^s : K \to K$ $(s \geqq 0)$* such that

$$\lambda^0(x) = 1,$$

$$\lambda^1(x) = x,$$

$$\lambda^s(x + y) = \sum_{t+r=s} \lambda^t(x) \cdot \lambda^r(y).$$

The results of Slepian (for $p = 2$) can be expressed by saying that $K(F)$ as a group is the free abelian group generated by indecomposable codes (a code is said to be indecomposable if it is not isomorphic to the sum of two smaller codes).

For a given code $C \subset V$ there are two functions of special interest:

1. $G_C(X) = \sum_{c \in C} X^{|c|} (= \sum \nu_s X^s$ where $\nu_s =$ the number of code points of weight s.)

2. $$Q_C(X) = \sum_{\xi \in V/C} X^{|\xi|}.$$

Here

$$|\xi| \overset{\text{def}}{=} \inf_{v \in \xi} |v|.$$

(ξ is a residue class of C in V and we have just described the quotient norm of $(V, |\cdot|)$ with respect to C.) It is easy to see that both Q and G define homomorphisms (*of groups*) $K(F) \xrightarrow{Q,G} \mathbf{Z}[[X]]_1^*$ ($\mathbf{Z}$ = the ring of integers). Thus we get a homomorphism

$$K(F) \xrightarrow{Q+G} \mathbf{Z}[[X]]_1^* \dotplus \mathbf{Z}[[X]]_1^*. \tag{24}$$

It is rather natural to conjecture that the kernel of this homomorphism is small, perhaps 0. If this is the case, then (24) gives a useful description of $K(F)$. It is perhaps interesting to study the problem of defining

a structure of a λ-ring on the group to the right in (24) so that $Q + G$ become a morphism for λ-rings.

Another problem: Is $K(F)$ generated as a λ-ring by some simple codes (e.g. cyclic codes?)?

Finally we may remark that there is some analogy between the theory of characteristic classes for vector bundles and the coefficients in Q_C and G_C.

RECEIVED: January 22, 1964

REFERENCES

BOREL, A. AND SERRE, J.-P. (1958), Le théorème de Riemann-Roch (d'après Grothendieck). *Bull. Soc. Math. France* **86**, 97–136.

GROTHENDIECK, A. (1958). La théorie des classes de Chern. *Bull. Soc. Math. France* **86**, 137–154.

LLOYD, S. P. (1957), Binary block coding. *Bell System Tech. J.* **36**, 517–535.

PETERSON, W. W. (1961), "Error-Correcting Codes." MIT Press, and Wiley, New York.

SLEPIAN, D. (1960), Some further theory of group codes. *Bell System Tech. J.* **39**, 1219–1252.

MACWILLIAMS, JESSIE (1963), A theorem on the distribution of weights in a systematic code. *Bell System Tech. J.* **42**, 79–94.